

# ACOS Venafi Integration Guide

February, 2024

#### © 2024 A10 Networks, Inc All rights reserved.

Information in this document is subject to change without notice.

#### PATENT PROTECTION

A10 Networks, Inc products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

#### TRADEMARKS

A10 Networks, Inc trademarks are listed at: a10-trademarks

#### DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc for current information regarding its products or services. A10 Networks, Inc products and services are subject to A10 Networks, Inc standard terms and conditions.

#### ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

#### FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc location, which can be found by visiting www.a10networks.com.

# **Table of Contents**

Overview	4
Integration with Venafi	5
Prerequisites	5
PowerShell Script Installation	6
Onboard Discovery of Applications and Certificates	8
Prerequisites	8
Creating an Onboard Discovery Job1	1
Executing the Onboard Discovery Job1	12
Certificate Renewal	L7
Prerequisites	17
Renewing Discovered Certificates1	8
Support2	20

### **Overview**

The creation or renewal of digital certificates involves several steps, multiple teams, and offers less visibility into expiring or noncompliant certificates.

Venafi demonstrates proven interoperability with A10 Thunder ADC to provide the customers with a consolidated and simplified method to manage critical security information, such as certificate locations, key sizes, ciphers used, and validity dates. This solution provides a complete view of an organization's digital certificates and makes it easy to fully automate the use of keys and certificates as the business grows.

The purpose of this document is to provide the steps to integrate A10 devices with Venafi Trust Protection Platform and automate certificate renewal. The overall process is described as follows:

- 1. Download and install the PowerShell script from the Venafi marketplace. See <u>PowerShell Script Installation</u>.
- 2. Create a Credential Object to authenticate the connection to the A10 device. See <u>Prerequisites</u>.
- 3. Create a Device object to reference the A10 device and validate its certificates and private keys. See <u>Prerequisites</u>.
- Create and execute an Onboard Discovery job to discover and import the applications and certificates into the Venafi platform. See <u>Creating an Onboard</u> <u>Discovery Job</u>.
- 5. Automate the renewal of expired certificates. The renewed certificates are downloaded and installed on the A10 device automatically. See <u>Certificate</u> <u>Renewal</u>.

The following topics are covered in this section:

Prerequisites	5
PowerShell Script Installation	6
Onboard Discovery of Applications and Certificates	8
Certificate Renewal	

### Prerequisites

Before performing the integration steps, ensure the following:

• Venafi Trust Protection Platform is installed and configured.

This platform rapidly develops an accurate certificate inventory and identifies security and operational risks.

- Connectivity between the Trust Protection Platform and Thunder device.
- A10 policy folder is created in the Venafi Trust Protection Platform.

It's a separate logical container for the A10 devices and policies inside the platform. To create the policy folder, see <u>Venafi documentation</u>.

• ACOS Thunder device is set up with a basic configuration.

In this document, it is assumed that the device is configured with a virtual server, having a virtual port with the Template Client SSL certificate associated with it.



# **PowerShell Script Installation**

You need to download and install the PowerShell script from the Venafi marketplace. This script provides routines that are invoked to conduct programmed operations in response to the Trust Protection Platform events at various phases of the certificate lifecycle.

To install the PowerShell script:

- 1. Go to the Venafi marketplace website.
- 2. Click Install Now (as shown in Figure 1).

Figure 1 : Venafi marketplace

V Venafi			PARTNERS	
Q Search App Store > App Details				
<b>A10</b>	A10 Networks Thunder ADC Updated Apr. 20 2022 HTTPS encryption is more prevalent than ever, but can be difficult to scale. A10 Networks get started and fully automate the use of keys and certificates as the organization grows	J <b>s</b> s and Venafi ha	Install No	ow te it easy to
	BUSINESS OUTCOMES  • Scale use of HTTPS without the difficult setup			
APPLICATION TYPE:	• Eliminate outages with continuous key and certificate updates			
App Security	INTEGRATION FEATURES <ul> <li>Onboard-discovery provides a complete machine identity inventory from the start</li> </ul>			
AVAILABILITY:	• Automate provisioning of renewed certificates			

- 3. Unzip the downloaded file.
- Place the script (A10\_Adaptable\_App.ps1) in the Program Files\Venafi\Scripts\AdaptableApp folder of your Venafi windows server instance.
- 5. Access Venafi Trust Protection Platform through the web browser.
- 6. From the menu bar, click **Policy Tree** and open the **A10** policy folder.
- 7. Navigate to Applications > Adaptable > Adaptable Settings > PowerShell Script.



8. Select A10\_Adaptable\_App script from the combo-box.

The A10 policy folder uses this script for all purposes.

A1	0 : Adaptab	le														$\leq$
	Applications	Certificate Trust Store	Cloud Instance Monitoring	Devices N	Vetwork Device Enrollment	Settings	View	General	Support							
+	Adaptable	Amazon AWS	Apache Azure Ker	Vault 🙆 Bas	sic BlueCoat SSLVA	CAPI	Citri	ix NetScaler	Connect:Direct	FS LTM Advanced	Google Cloud Load Balancer	IBM DataPower	IBM IBM GSK	EImperva MX	<b>I</b> JKS	@0rz +
															4	Print 🗳
	General															
					4	Contact(s):	local:tpp	padmin (\VI	ED\Identity\tppadm	lin)					5	
					Ac	pprover(s):	local:tpp	padmin (\VI	ED\Identity\tppadm	in)					8.	
					Ma	anaged By:							0		0 -	
l																
	Application In	formation														-
					Application	Credential:	_								1.	1
					Secondary	Credential:	-								1	
					Secondary .	creation.										
						Port:	443									
	Adaptable Set	tings			_				_							
					PowerS	hell Script:	A10,Adap	ptable_App					0		- 52	
			When script is up	dated, fix related	d provisioning and discov	ery errors:	Yes					0			0 -	
					Private Key	Credential:	L .								1.	
					Port Number (De	fault 443):	*								1 -	
					VPort Protocol (Defau	ult HTTPS):									0 -	
						Partition:									0.	
					Private Key PBE	Algorithm:	High sec	urity but low sy	rstem compatibility (SHA)	56 AE\$256)			0		1.	
							Each alg	gorithm type	has a corresponding s	ecurity/compatibility value	e. Generally, they are inversely related	ted due to their adoptio	n by soft-			



# **Onboard Discovery of Applications and Certificates**

The Onboard Discovery feature automates the process of importing certificates from the A10 devices into the Trust Protection Platform so you can monitor, validate, and provision them.

This section describes the steps to create and execute an Onboard Discovery job.

The following topics are covered:

Prerequisites	8
Creating an Onboard Discovery Job	11
Executing the Onboard Discovery Job	15

### Prerequisites

Before running the onboard discovery job, ensure the following tasks are performed:

1. Create a credential object on the Trust Protection Platform to authenticate the A10 device.

To create a credential object:

- a. Open the **Policy Tree** view.
- b. Click A10 policy and right click to select Add > Credential > Username Credential.

#### Integration with Venafi



Search options F Belicy Administration
 Solution General 🖃 晏 Venafi Internal 🗄 🌄 Certs H Goveloper Environments 🗄 晏 Intune 🗄 🌄 SA B SCEP E \_\_\_\_\_CA Template Testing Log View 📲 🍃 纋 Open 🐺 Open in New Window ±. 🕂 Add Certificates • ± 2 Rermissions • Devices . • GA Template 🔹 Refresh ± 4 Policy 🗉 🛃 🖺 Expand All Collapse All R Credential . 🔏 Amazon Credential • & Workflow 2 Certificate Credential 🗄 🚽 耳 Rename Ceneric Credential Aperture Configuration • A Move • AWS EC2 Instance Monitor Roogle Credential 🗄 🚽 🗙 Delete 🛃 Certificate Trust Bundle Password Credential E 🗄 🌄 PrimeKey 🔏 Private Key Credential 🗄 璗 QuoVadis Username Credential 🗄 🌄 Radware H SVault Test

The Username Credential page is displayed (Figure 2).

Figure 2 : Username Credential page

Add New : Username Credential		
General		
General	* Credential Name: A10 API liser	
	Description:	
	Contact(s):	
Settings		
	* Expires: 3/22/2032	
Credential		
	* User Name: venafi	
	* Password:	
	* Confirm Password:	

- c. In the **General** section, enter a credential object name in the **Credential Name** field.
- d. In the **Credential** section, enter a username and password in the respective fields.





**NOTE:** Enter the same credentials that are used to login to the A10 Thunder device.

- e. Click Save.
- 2. Create a device object on the Trust Protection Platform to reference the A10 device and validate its certificates and private keys.

To create a device object:

- a. Open the **Policy Tree** view.
- b. Click **A10** policy and right click to select **Add > Devices > Device**.



The **Device** page is displayed (Figure 3).

••••



#### Figure 3 : Device page

ad New : Device		
		Print
General		9
* Device Name:	Test A10 Device	
Description:		
Contact(s):	local:tppadmin (\VED\Identity\tppadmin)	<b>.</b>
Host Information		-
Hostname/Address:	129.146.202.33	
Provisioning Mode:	Agentiess	1 .
Concurrent Connection Limit:	1	0 -
Device Credential:	VVED\Policy/Venafi Internal\Testing\A10\A10 API User	0 -
Temp Directory:		1.
OS Type:	Automatic B	0 -
Jump Server:		0 -
Use Sudo:	No	0 -
Sudo Credential (optional):		1.
Enforce Host Key:	N0 0	1.
Presented Thumbprint:		
Presented Key Type:		

- c. In the General section, enter a name in the Device Name field.
- d. In the **Host Information** section, enter the IP address of the A10 device.
- e. In the **Device Credential** field, specify the credential object (created in <u>Step 1</u>). This object is used to authenticate the connection with the A10 device.
- f. Click Save.

For more information, see <u>Device Object Setting</u>.

### Creating an Onboard Discovery Job

To create an Onboard Discovery job:

1. Open the **TLS Protect** management interface on the Trust Protection Platform.

Dashboar	ds - Venafi Ser	vers Poli	icy Tree E	ncryption	Notifications	API ~	Client	ts ~	Logs				~		0		PC
10 : Adapt	able												YC	UR PR	ODUCTS		<
Applications	Certificate Trust Store	Cloud Instano	e Monitoring	Devices	Network Device Enrollment	Settings	View	General	Support					🕡 т	LS Protect		
🖌 Adapta	ble Amazon AWS	Apache	Azure Key Va	uit 🙆 B	lasic DBlueCoat SSLVA	CAPI	Citr	ix NetScaler	Connect:Direct	F5 LTM Advanced	Google Cloud Load Balancer	IBM DataPower	IBM G	Q, s	SH Protect	_	Print
General														4 c	odeSign Prote	ect	-
						Contact(s):	local:tp	padmin (\V	/ED\Identity\tppadm	in)				0 c	lient Protect		
					A	pprover(s): anaged By:	local:tp	padmin (\V	VED\Identity\tppadm	in)				P	latform	~	

2. Navigate to **Configuration > Jobs**.

#### Integration with Venafi



VENAFI	守 TLS Protect	Dashboards ~	Inventory ~	Policy Tree	Reports ~	Configuration ^	Clients ~	Workflow ~ I	.ogs
All Certificates	Dashboard					Custom Fields Placement Rules	00		
Certificate Tot	als +					Notifications			
My Certificates	Expiring wit days	thin 30 In Erro	r	Key Size < 2048 RSA keys	Weak Sig Algorithm	Jobs	>	Unapproved Issuer	Pen App
30,63	90 S	9	579	0		CA Templates	6	30,581	
						ACME			
Key Size					Signing Alg	Folders			

3. Click + Create New Job to start the Create New Job wizard.

VENAFI	TLS Protect Dashboards ~	Inventory V Policy Tree	Reports ~ Configurati	on - Clients - Workfle	ow ~ Logs			۹	0 🏼 🖻
Jobs								ħ	+ Create New Job
Jobs Filters		✓ Change Job Priority							0 Jobs
Job Type		Job Name #	Status P	Next Run 7	Last Run 🕫	Туре 🕫	Results	Priority =	
Status									
Last Run									
m									
	Clea	ir all							

4. On the Create New Job page, select Onboard Discovery, and then click Start.



• • •<mark>•</mark> • • •



#### The Job Details page is displayed.

Name *				
Discover A10				
Description				
Contacts				
Search for an identity	-			
Installation Type *				
Adaptable				
💋 Enable Debug Loggin	3			

- 5. In the Name field, enter a name for your new onboard discovery job.
- 6. In the **Description** field, enter a description that describes the purpose for this new job (this is optional).
- 7. In the **Contacts** field, enter the contact names for your new job (this is optional).
- 8. In the **Installation Type** list field, select the installation type as **Adaptable** and click **Next**.

The **Targets** page is displayed.

Devices to Scan		Create New Devices
Policy \ Venafi Internal \ Testing \	A10 \ Test A10 Device ×	
Scan all Devices located in this fol	lder (and its subfolders)	
Scan all Devices located in this for Search	lder (and its subfolders)	~

9. In the **Devices to Scan** field, select the device object created <u>previously</u> and click **Next**.



The **Placement Rules** page is displayed.

Next, let's define the placement rules for your Onboard Discovery job.

Diago no	why discovere	d cortificator	
Flace ne	wiy discovere	d certificates	
O With	this device	In this folder	

- 10. On the Placement Rules page, select one of the following,
  - With this device Stores all the newly discovered certificates in the same folder where the device is located.
  - In this folder Stores all the newly discovered certificates in the folder you specify (in the field below).
- 11. Click Next.

The Run Time page is displayed.

Run Ti	me (All times a	are local)	
Frequen	cv *		
🗸 Manua	lly run		¢
Every	week		
Every	month		
Every	vear 📐		

12. On the **Run Time** page, set the **Frequency** for running the job by selecting one of the following,

14



- Every week / Every month / Every year Sets a recurring time for the job to regularly synchronize the inventories by discovering newly added certificates.
- Manually run Executes the job manually whenever required.
- 13. Click Create Job.

The job is created and displayed under the jobs list on the **Jobs** page.

Jobs									+ Create New Job
Jobs Filters Job Type	~	Change Job Priority	Status =	Next Run 7	Last Run 7	Type 7	Results	Priority =	1 Job
Status		Discover A10		Manual	Never	Onboard Discovery Adaptable	Certificates: 0		Run Now *
Last Run									
	Clear all								

### Executing the Onboard Discovery Job

To execute the discovery job:

1. After the job is created and displayed on the Jobs page, click Run Now.

Jobs								+ Create New Job
Jobs Filters V	Change Job Priority	Status 7	Next Run =	Last Run 7	Type =	Results	Priority =	1 Job
Status	Discover A10		Manual	Never	Onboard Discovery Adaptable	Certificates: 0		Run Now *
Last Run								
Ciear all								

When the execution is complete, the Discovery page displays the Status as Complete. Additionally, the New Applications and New Certificates fields display the number of applications and certificates discovered on the device.

#### Integration with Venafi



Discover A10		
Results Details and Targets Schedule	Results	Complete
Permissions	Status Last Run New Applications	3/22/2022 8:46 AM (-07:00 UTC) 1
	New Keys	0
	Devices	
	Pending	0
	In Progress	0
	Failed	0
	Completed	1
	Aborted	0

2. To view the newly discovered applications and associated certificates, switch to the Policy Tree view and refresh it.



**NOTE:** During onboard discovery, only the public section of the certificates and the metadata required for provisioning the certificates are imported. The Venafi Trust Protection Platform does not import or store the private key.

. . . . . . . . .



# Certificate Renewal

Certificate renewal is the process of purchasing a new certificate for the same public key that was used in the expired certificate. After renewal, the new certificate is automatically downloaded and installed on the device.

This section describes the steps to renew the expired certificates.

The following topics are covered:

Prerequisites	.17
Renewing Discovered Certificates	. 18

### Prerequisites

Before renewing the certificates, ensure that the **Certificate Authority (CA) template** is configured under the A10 certificate policy (as shown in the figure below). For steps to create and configure the Certification Authority (CA) template, see <u>Configuring Certificate Authority</u>.

Policy \$	A10 : Certificate	
📲 Add • 🗙 Delete Show all • 🗳	Applications Certificate Trust Store Cloud Instance Monitoring Devices Rietwork Device Enrollment. Settings View General Support	
204	😡 Policy 🔬 Cerefrate 📓 Certificate Authorities 🔮 Certificate True: Bundle 🕺 Certificate True: Bundle 🕺 Certificate True: Bundle	
Search options		@ Print
🗄 🥪 Policy	Allow Wildcards: Yes	
B Administration	Allow Duplicate Common and Subject Alternative Names: Yes	
S Venati Internal		
B Certs	Private Key	9
B      Developer Environments	Reuse Private Key for Service Generated CSRs: No B	0.
a 🤯 sa	Allow Users to Import Duplicate Certificates and Reuse Private Keys: Nn 😝	1.
B SCEP	Key Algorithm: R1A 6	1.
and _and and a fing	Key Strength (bits): 2045	1.
A10	Eliptic Curve: (2255	2.
🗃 👹 Test A10 Device		
A10 API User	Other Information	8
H AN	CA Templates: \Papilov\Administration\CA Templates\MSCA - I Year SSL	<b>Q</b> .
Cert Storage	Key Generation: Software 8	1.
Credential Testing	Encryotion Key: Software Datasit	1.
B CSC Global	Disable Automatic Revenue: No B	11-
B F5	Allow Simple Passwards for Private Key Downloads: No B	1.
H F5 Silverline	Private Key PBE Algorithm: Insecure but good switten compatibility (MDS DES)	
B Glabalsian	Each algorithm type has a corresponding security/compacibility value. Generally, they are inversely related due to their adoption by soft-	
HashiCorp	ware applications.	
HydrantiD	Refewal Window: 30 dbys	<b>/</b> •

The CA template object contains information required for the Trust Protection Platform to connect to the CA for certificate management.

Additionally, the certificate renewal behavior is affected by certain options configured under the A10 Certificate policy. Hence, ensure that the following options are configured correctly,

17



- **Disable automatic renewal**: By default, automatic renewal is enabled for certificates in the Trust Protection Platform. To disable automatic renewal, set this value to **Yes**.
- **Renewal window**: This parameter indicates the number of days before expiration, to renew the certificates. It is recommended to set this value between 30 to 90 days to ensure that there is enough time to complete the processes and necessary approvals for renewing the certificate before the old certificate expires.

### **Renewing Discovered Certificates**

To renew the discovered certificate:

1. Open the certificate in the **Policy Tree** view and click **Renew Now**.

art   🌾 Retry   🎲 Reset · oficate Status	Renew Now Scheck Revocati	on   💞 Validate Now   🔬 Revoke 🔹   🍓 Cho	ange Certificate Type				\$
OK Expiration Date 3/18/2023 1:44:27 PM				Lifecycle Stage none Validation Last Check: never SSL/T	LS Result:		
Result: Revoca	tion check not yet attempted			State: F	ile Result:		
Result: Revoca	tion check not yet attempted			State: F	ile Result:		
Result: Revoca	tion check not yet attempted Application	Installation Status	Stage	State: F	ile Result: SSL/TLS Validation Result	File Validation Result	
Result: Revoca	tion check not yet attempted Application yz=1	Installation Status OK	Stage	State: F	SSL/TLS Validation Result	File Validation Result	

2. On the confirmation pop-up, click **Yes** to commence the certificate renewal process.

Vould you like to renow th	is cortificate now?
vouid you like to reliew d	is certificate now:

The following processes take place in the background:

- a. The Trust Protection Platform creates a private key and generates the certificate signing request (CSR).
- b. The CSR is forwarded to the configured Certificate Authority (CA).



- c. The Trust Protection Platform retrieves the new signed certificate and key from the CA.
- d. The new signed certificate and private key is sent to the A10 device and installed automatically.
- 3. Verify new certificate installation by checking the certificate information in the A10 interface.
  - A. To check the renewed certificate information, navigate to ADC > SSL Management > SSL Certificates.

Cort Respection List	Exercise Email	CMR Codification ACI	IE Certificator						vThunder	520 build
Cent Revocation List	Expiration Email	CMP Germales AGN	re Germoates						*THURDON	5.4.0, Duna
/ SSL Management / SSL Cer	tificates									
									_	
Search for Certificate Name		Q Search C Rese	đ			C Refresh	📋 Delete	+ Create	≧Import	AExport .
SSL Certificate Name	Туре	Common Name	Organization	Expiration	Issuer					Actions
vs-1_23mar18_233D	certificate/key	vs-1		Mar 18 19:44:27 2023 GMT	/DC=com/DC=venafidemo/CN=venafidemo-TPP-CA					Export -
vs-2test_23mar18_233E-1	certificate	venafidemo-TPP-CA		Oct 17 15:57:49 2024 GMT	/DC=com/DC=venafidemo/CN=venafidemo-TPP-CA					Export-
vs-1_23mar22_23F1-1	certificate	venafidemo-TPP-CA		Oct 17 15:57:49 2024 GMT	/DC=com/DC=venafidemo/CN=venafidemo-TPP-CA					Export -
vs-2test_23mar18_233E	certificate/key	vs-2test		Mar 18 20:04:25 2023 GMT	/DC=com/DC=venafidemo/CN=venafidemo-TPP-CA					Export -
vs-1_23mar18_233D-1	certificate	venafidemo-TPP-CA		Oct 17 15:57:49 2024 GMT	/DC=com/DC=venafidemo/CN=venafidemo-TPP-CA					Export-
venati	certificate/key	cavisson	A10	Feb 13 17:53:02 2022 GMT	/C=US/ST=California/L=SANJose/O=A10/OU=QA/CN=cavisson/ema	ilAddress=rezae	@a1			Export -
vs-1_23mar22_23F1	certificate/key	vs-1		Mar 22 15:44:22 2023 GMT	/DC=com/DC=venafidemo/CN=venafidemo-TPP-CA					Export -
vs-1_23mar18_233D_key	key									Export
vs-2test_23mar18_233E_key	key									Export
vs-1_23mar22_23F1_key	key									Export
default ca bundle	CA-Certificate	GlobalSign Root CA	GlobalSign nv-sa	Jan 28 12:00:00 2028 GMT	/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA					Export -

B. The renewed certificate is also associated with the virtual port configuration replacing the old certificate. To check this config, navigate to ADC > SLB > Virtual Server > Virtual Port > Edit > Template Client SSL.

Servers Virtual Services Service Groups Servers	Policy Limits Application Global Session Resource Usage	vThunder 5.2.0, build
SLB / Virtual Servers / vs-1 / Virtual Port / Upo	lato	
odate Virtual Port		
Manua		
Protocol *		
Port or Port Range *	ntps	
Connection Limit	443	
Action	Enable	•
Support HTTP2		
Source NAT Pool		
Source NAT Auto		
Source NAT Use CGNv6		
Service Group	sg-1	¢ Add+
Femplate Cilent SSL	vs-1_23mar22_23F1	+ Add+
Template Server SSL		* Add+
emplate Cache		¢ Add+
Template HTTP		÷ Add+
Persist Type	Obstination IP O Source IP O Cookle	
	Advanced Fields	
	Terrelates	
	Templates	
	rempiates	

For more information, see <u>Certificate Renewal</u>.

# Support

For more information about A10 Thunder products, contact A10 Networks at: <a href="https://www.a10networks.com/contact-us/">https://www.a10networks.com/contact-us/</a>.

For technical assistance, contact A10 Networks Technical Support by following the instructions at: <u>https://support.a10networks.com/</u>.



©2024 A10 Networks, Inc All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.